

PARENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

United States Patent and Trademark
Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 12 April 1999 (12.04.99)	in its capacity as elected Office
International application No. PCT/US98/17321	Applicant's or agent's file reference 3220-60866
International filing date (day/month/year) 21 August 1998 (21.08.98)	Priority date (day/month/year) 22 August 1997 (22.08.97)
Applicant	
GLOGAU, Jordan, J. et al	

1. The designated Office is hereby notified of its election made:

in the demand filed with the International Preliminary Examining Authority on:

08 March 1999 (08.03.99)

in a notice effecting later election filed with the International Bureau on:

2. The election was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

<p>The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland</p> <p>Facsimile No.: (41-22) 740.14.35</p>	<p>Authorized officer</p> <p>Céline Faust</p> <p>Telephone No.: (41-22) 338.83.38</p>
---	---

PCT**REQUEST**

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

International Application No.

International Filing Date

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference
(if desired) (12 characters maximum)

3220-60866

Box No. I TITLE OF INVENTION**DATA HIDING****Box No. II APPLICANT**

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

PURDUE RESEARCH FOUNDATION
1021 Hovde Hall, Room 307
West Lafayette, Indiana 47907-1021
US

 This person is also inventor.Telephone No.
(765) 494-2610Facsimile No.
(765) 496-1277

Teleprinter No.

State (that is, country) of nationality:

US

State (that is, country) of residence:

US

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

GLOGAU, Jordan J.
271 Treetop Circle
Nanuet, New York 10954
US

This person is:

 applicant only applicant and inventor inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

US

State (that is, country) of residence:

US

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

 Further applicants and/or (further) inventors are indicated on a continuation sheet.**Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE**

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:

 agent common representative

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)

NIEDNAGEL, Timothy E.
BARNES & THORNBURG
11 South Meridian Street
Indianapolis, Indiana 46204
US

Telephone No.

(317) 236-1313

Facsimile No.

(317) 231-7433

Teleprinter No.

Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Continuation of Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

If none of the following sub-boxes is used, this sheet should not be included in the request.

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

DELP, Edward J. III
400 Evergreen Street
West Lafayette, Indiana 47906
US

This person is:

applicant only
 applicant and inventor
 inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

US

State (that is, country) of residence:

US

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

WOLFGANG, Raymond B.
404 Longwood Drive
Exton, Pennsylvania 19341
US

This person is:

applicant only
 applicant and inventor
 inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

US

State (that is, country) of residence:

US

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

LIN, Eugene Ted
3303 Hunger Road
West Lafayette, Indiana 47906
US

This person is:

applicant only
 applicant and inventor
 inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

US

State (that is, country) of residence:

US

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

This person is:

applicant only
 applicant and inventor
 inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

State (that is, country) of residence:

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

Further applicants and/or (further) inventors are indicated on another continuation sheet.

Box No.V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) (mark the applicable check-boxes; at least one must be marked):

Regional Patent

AP ARIPO Patent: GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, SD Sudan, SZ Swaziland, UG Uganda, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT

EA Eurasian Patent: AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT

EP European Patent: AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT

OA OAPI Patent: BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT (if other kind of protection or treatment desired, specify on dotted line)

National Patent (if other kind of protection or treatment desired, specify on dotted line):

<input type="checkbox"/> AL Albania	<input type="checkbox"/> LS Lesotho
<input type="checkbox"/> AM Armenia	<input type="checkbox"/> LT Lithuania
<input type="checkbox"/> AT Austria	<input type="checkbox"/> LU Luxembourg
<input type="checkbox"/> AU Australia	<input type="checkbox"/> LV Latvia
<input type="checkbox"/> AZ Azerbaijan	<input type="checkbox"/> MD Republic of Moldova
<input type="checkbox"/> BA Bosnia and Herzegovina	<input type="checkbox"/> MG Madagascar
<input type="checkbox"/> BB Barbados	<input type="checkbox"/> MK The former Yugoslav Republic of Macedonia
<input type="checkbox"/> BG Bulgaria	<input type="checkbox"/> MN Mongolia
<input type="checkbox"/> BR Brazil	<input type="checkbox"/> MW Malawi
<input type="checkbox"/> BY Belarus	<input type="checkbox"/> MX Mexico
<input type="checkbox"/> CA Canada	<input type="checkbox"/> NO Norway
<input type="checkbox"/> CH and LI Switzerland and Liechtenstein	<input type="checkbox"/> NZ New Zealand
<input type="checkbox"/> CN China	<input type="checkbox"/> PL Poland
<input type="checkbox"/> CU Cuba	<input type="checkbox"/> PT Portugal
<input type="checkbox"/> CZ Czech Republic	<input type="checkbox"/> RO Romania
<input type="checkbox"/> DE Germany	<input type="checkbox"/> RU Russian Federation
<input type="checkbox"/> DK Denmark	<input type="checkbox"/> SD Sudan
<input type="checkbox"/> EE Estonia	<input type="checkbox"/> SE Sweden
<input type="checkbox"/> ES Spain	<input type="checkbox"/> SG Singapore
<input type="checkbox"/> FI Finland	<input type="checkbox"/> SI Slovenia
<input type="checkbox"/> GB United Kingdom	<input type="checkbox"/> SK Slovakia
<input type="checkbox"/> GE Georgia	<input type="checkbox"/> SL Sierra Leone
<input type="checkbox"/> GH Ghana	<input type="checkbox"/> TJ Tajikistan
<input type="checkbox"/> GM Gambia	<input type="checkbox"/> TM Turkmenistan
<input type="checkbox"/> GW Guinea-Bissau	<input type="checkbox"/> TR Turkey
<input type="checkbox"/> HR Croatia	<input type="checkbox"/> TT Trinidad and Tobago
<input type="checkbox"/> HU Hungary	<input type="checkbox"/> UA Ukraine
<input type="checkbox"/> ID Indonesia	<input type="checkbox"/> UG Uganda
<input type="checkbox"/> IL Israel	<input checked="" type="checkbox"/> US United States of America
<input type="checkbox"/> IS Iceland	<input type="checkbox"/> UZ Uzbekistan
<input checked="" type="checkbox"/> JP Japan	<input type="checkbox"/> VN Viet Nam
<input type="checkbox"/> KE Kenya	<input type="checkbox"/> YU Yugoslavia
<input type="checkbox"/> KG Kyrgyzstan	<input type="checkbox"/> ZW Zimbabwe
<input type="checkbox"/> KP Democratic People's Republic of Korea	
<input type="checkbox"/> KR Republic of Korea	
<input type="checkbox"/> KZ Kazakhstan	
<input type="checkbox"/> LC Saint Lucia	
<input type="checkbox"/> LK Sri Lanka	
<input type="checkbox"/> LR Liberia	

Check-boxes reserved for designating States (for the purposes of a national patent) which have become party to the PCT after issuance of this sheet:

.....

.....

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. (Confirmation of a designation consists of the filing of a notice specifying that designation and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.)

Box No. VI PRIORITY CLAIM		<input type="checkbox"/> Further priority claims are indicated in the Supplemental Box.		
Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is:		
		national application: country	regional application: regional Office	international application: receiving Office
item (1) (22.08.97) 22 August 1997	60/056,724	US		
item (2)				
item (3)				

The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) (only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office) identified above as item(s): **(1)**

* Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) (if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used): ISA / EP	Request to use results of earlier search; reference to that search (if an earlier search has been carried out by or requested from the International Searching Authority): Date (day/month/year)	Number	Country (or regional Office)
---	---	--------	------------------------------

Box No. VIII CHECK LIST; LANGUAGE OF FILING

This international application contains the following number of sheets: request : 4 description (excluding sequence listing part) : 11 claims : 4 abstract : 1 drawings : 4 sequence listing part of description : 0 Total number of sheets : 24	This international application is accompanied by the item(s) marked below: 1. <input checked="" type="checkbox"/> fee calculation sheet 2. <input checked="" type="checkbox"/> separate signed power of attorney (4) 3. <input checked="" type="checkbox"/> copy of general power of attorney; reference number, if any: 4. <input type="checkbox"/> statement explaining lack of signature 5. <input type="checkbox"/> priority document(s) identified in Box No. VI as item(s): 6. <input type="checkbox"/> translation of international application into (language): 7. <input type="checkbox"/> separate indications concerning deposited microorganism or other biological material 8. <input type="checkbox"/> nucleotide and/or amino acid sequence listing in computer readable form 9. <input checked="" type="checkbox"/> other (specify): Transmittal Letter to the RO/US Return Postal Card
--	---

Figure of the drawings which should accompany the abstract: **4** Language of filing of the international application: **English**

Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

Timothy E. Niednaqel, Agent for Applicants

For receiving Office use only

1. Date of actual receipt of the purported international application:	2. Drawings: <input type="checkbox"/> received: <input type="checkbox"/> not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:	
4. Date of timely receipt of the required corrections under PCT Article 11(2):	
5. International Searching Authority (if two or more are competent): ISA /	6. <input type="checkbox"/> Transmittal of search copy delayed until search fee is paid.

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

PCT

GENERAL POWER OF ATTORNEY (for several international applications filed under the Patent Cooperation Treaty) (PCT Rule 90.5)

The undersigned person(s) :

(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)

PURDUE RESEARCH FOUNDATION
1021 Hovde Hall, Room 307
West Lafayette, Indiana 47907-1021
US

hereby appoint(s) the following person as:

agent

common representative

Name and address

(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)

LAMMERT, Steven R.; COFFEY, William R.; HYLAND, Jerry E.; CONARD, Richard D.; REZEK, Richard A.; NIEDNAGEL, Timothy E.; BRENN, John P.; WOODBURN, Jill L.; HARRISON, Nancy, J.; CARTER, R. Trevor; KULKARNI, Dilip A.; PALAN, Perry; NEWMAN, Mark M.; GILLENWATER, Bobby B.; HUNT, Paul B.; GZYBOWSKI, Michael S.; GALLAGHER, Gerald T.; NULL, Robert D.;

All Appointed Agents of the Address:

BARNES & THORNBURG
11 South Meridian Street
Indianapolis, Indiana 46204
US

to represent the undersigned before

all the competent International Authorities

the International Searching Authority only

the International Preliminary Examining Authority only

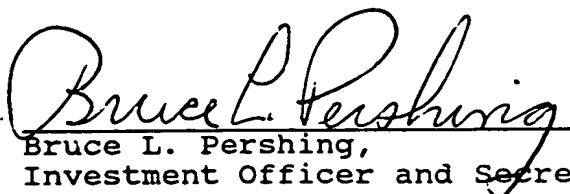
in connection with any and all international applications filed by the undersigned with the following Office

US

as receiving Office

and to make or receive payments on behalf of the undersigned.

Signature(s) (where there are several persons, each of them must sign; next to each signature, indicate the name of the person signing and the capacity in which the person signs, if such capacity is not obvious from reading this power):


Bruce L. Pershing,
Investment Officer and Secretary

Date:

(14.07.98)
14 July 1998
Day/ Month/ Year

PCT

POWER OF ATTORNEY

(for an international application filed under the Patent Cooperation Treaty)

(PCT Rule 90.4)

The undersigned applicant(s) (Names should be indicated as they appear in the request):

GLOGAU, Jordan J.
271 Treetop Circle
Nanuet, New York 10954
US

hereby appoints (appoint) the following person as:

agent

common representative

Name and address

(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)
NIEDNAGEL, Timothy E.; COFFEY, William R.; HYLAND, Jerry E.; BARNES, D.; LAMMERT, Steven R.; REZEK, Richard A.; BREEN, John P.; WOODBURN, Jill L.; HARRISON, Nancy, J.; CARTER, R. Trevor; KULKARNI, Dilip A.; PALAN, Perry; NEWMAN, Mark M.; GILLENWATER, Bobby B.; HUNT, Paul B.; GZYBOWSKI, Michael S.; GALLAGHER, Gerald T.; NULL, Robert D.

All Appointed Agents of the Address:

BARNES & THORNBURG
11 South Meridian Street
Indianapolis, Indiana 46204
US

to represent the undersigned before

all the competent International Authorities

the International Searching Authority only

the International Preliminary Examining Authority only

in connection with the international application identified below:

Title of the invention: DATA HIDING

Applicant's or agent's file reference: 3220-60866

International application number (if already available): PCT/US98/

filed with the following Office US as receiving Office
and to make or receive payments on behalf of the undersigned.

Signature of the applicant(s) (where there are several applicants, each of them must sign; next to each signature, indicate the name of the person signing and the capacity in which the person signs, if such capacity is not obvious from reading the request or this power):

Jordan J. GLOGAU

Date: 12 8 98
Day/ Month/ Year

PCT

POWER OF ATTORNEY

(for an international application filed under the Patent Cooperation Treaty)

(PCT Rule 90.4)

The undersigned applicant(s) (Names should be indicated as they appear in the request):

DELP, Edward J. III
400 Evergreen Street
West Lafayette, Indiana 47906
US

hereby appoints (appoint) the following person as: agent common representative

Name and address

(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)
NIEDNAGEL, Timothy E.; COFFEY, William R.; HYLAND, Jerry E.; CONARD, Richard D.; LAMMERT, Steven R.; REZEK, Richard A.; BREEN, John P.; WOODBURN, Jill L.; HARRISON, Nancy, J.; CARTER, R. Trevor; KULKARNI, Dilip A.; PALAN, Perry; NEWMAN, Mark M.; GILLENWATER, Bobby B.; HUNT, Paul B.; GZYBOWSKI, Michael S.; GALLAGHER, Gerald T.; NULL, Robert D.;
All Appointed Agents of the Address:

BARNES & THORNBURG
11 South Meridian Street
Indianapolis, Indiana 46204
US

to represent the undersigned before

all the competent International Authorities
 the International Searching Authority only
 the International Preliminary Examining Authority only

in connection with the international application identified below:

Title of the invention: DATA HIDING

Applicant's or agent's file reference: 3220-60866

International application number (if already available): PCT/US98/

filed with the following Office US as receiving Office
and to make or receive payments on behalf of the undersigned.

Signature of the applicant(s) (where there are several applicants, each of them must sign; next to each signature, indicate the name of the person signing and the capacity in which the person signs, if such capacity is not obvious from reading the request or this power):


Edward J. DELP III

(14.08.98)

Date: 14 August 1998
Day/ Month/ Year

PCT

POWER OF ATTORNEY (for an international application filed under the Patent Cooperation Treaty) (PCT Rule 90.4)

The undersigned applicant(s) (Names should be indicated as they appear in the request):

WOLFGANG, Raymond B.
404 Longwood Drive
Exton, Pennsylvania 19341
US

hereby appoints (appoint) the following person as: agent common representative

Name and address

(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)

NIEDNAGEL, Timothy E.; COFFEY, William R.; HYLAND, Jerry E.; CONARD, Richard D.; LAMMERT, Steven R.; REZEK, Richard A.; BREEN, John P.; WOODBURN, Jill L.; HARRISON, Nancy, J.; CARTER, R. Trevor; KULKARNI, Dilip A.; PALAN, Perry; NEWMAN, Mark M.; GILLENWATER, Bobby B.; HUNT, Paul B.; GZYBOWSKI, Michael S.; GALLAGHER, Gerald T.; NULL, Robert D.

All Appointed Agents of the Address:

BARNES & THORNBURG
11 South Meridian Street
Indianapolis, Indiana 46204
US

to represent the undersigned before

all the competent International Authorities
 the International Searching Authority only
 the International Preliminary Examining Authority only

in connection with the international application identified below:

Title of the invention: DATA HIDING

Applicant's or agent's file reference: 3220-60866

International application number (if already available): PCT/US98/

filed with the following Office US as receiving Office
and to make or receive payments on behalf of the undersigned.

Signature of the applicant(s) (where there are several applicants, each of them must sign; next to each signature, indicate the name of the person signing and the capacity in which the person signs, if such capacity is not obvious from reading the request or this power):


Raymond B. Wolfgang

(11.08.98)
Eleven August 1998

Date: 8-11-98
Day / Month / Year

PCT

POWER OF ATTORNEY

(for an international application filed under the Patent Cooperation Treaty)

(PCT Rule 90.4)

The undersigned applicant(s) (Names should be indicated as they appear in the request):

LIN, Eugene Ted
3303 Hunter Road
West Lafayette, Indiana 47906
US

hereby appoints (appoint) the following person as:

agent

common representative

Name and address

(Family name followed by given name: for a legal entity, full official designation. The address must include postal code and name of country.)

NIEDNAGEL, Timothy E.; COFFEY, William R.; HYLAND, Jerry E.; CONARD, Richard D.; LAMMERT, Steven R.; REZEK, Richard A.; BRENN, John P.; WOODBURN, Jill L.; HARRISON, Nancy, J.; CARTER, R. Trevor; KULKARNI, Dilip A.; PALAN, Perry; NEWMAN, Mark M.; GILLENWATER, Bobby B.; HUNT, Paul B.; GZYBOWSKI, Michael S.; GALLAGHER, Gerald T.; NULL, Robert D.; All Appointed Agents of the Address:
BARNES & THORNBURG
11 South Meridian Street
Indianapolis, Indiana 46204
US

to represent the undersigned before

all the competent International Authorities

the International Searching Authority only

the International Preliminary Examining Authority only

in connection with the international application identified below:

Title of the invention: DATA HIDING

Applicant's or agent's file reference: 3220-60866

International application number (if already available): PCT/US98/

filed with the following Office US as receiving Office
and to make or receive payments on behalf of the undersigned.

Signature of the applicant(s) (where there are several applicants, each of them must sign; next to each signature, indicate the name of the person signing and the capacity in which the person signs, if such capacity is not obvious from reading the request or this power):

Eugene Ted LIN
Eugene Ted LIN

Date: 12 / 8 / 98
Day/ Month/ Year

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



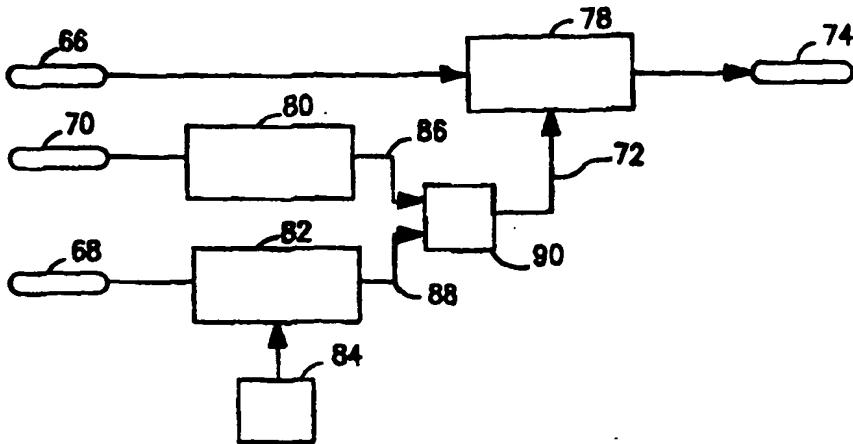
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 9/00, H04N 1/32		A1	(11) International Publication Number: WO 99/11020
			(43) International Publication Date: 4 March 1999 (04.03.99)
(21) International Application Number: PCT/US98/17321		(81) Designated States: JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 21 August 1998 (21.08.98)		Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>	
(30) Priority Data: 60/056,724 22 August 1997 (22.08.97) US			
(71) Applicant (for all designated States except US): PURDUE RESEARCH FOUNDATION [US/US]; 1021 Hovde Hall, Room 307, West Lafayette, IN 47907-1021 (US).			
(72) Inventors; and			
(75) Inventors/Applicants (for US only): GLOGAU, Jordan, J. [US/US]; 271 Treetop Circle, Nanuet, NY 1054 (US). DELP, Edward, J., III [US/US]; 400 Evergreen Street, West Lafayette, IN 47906 (US). WOLFGANG, Raymond, B. [US/US]; 404 Longwood Drive, Exton, PA 19341 (US). LIN, Eugene, Ted [US/US]; 3303 Hunter Road, West Lafayette, IN 47906 (US).			
(74) Agent: NIEDNAGEL, Timothy, E.; Barnes & Thornburg, 11 South Meridian Street, Indianapolis, IN 46204 (US).			

(54) Title: HIDING OF ENCRYPTED DATA

(57) Abstract

A method of data hiding includes providing a message (68), providing an encrypting sequence (86), and generating an encrypted message (72) based on the message and the encrypting sequence. A carrier signal (66) that conveys information unrelated to the encrypted message is provided, and the encrypted message is embedded (78) into the carrier signal by performing an exclusive-OR of the encrypted message with a first portion of the carrier signal.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

HIDING OF ENCRYPTED DATA

Field of the Invention

The present invention relates to methods and apparatus for hiding data
5 within a digital signal, and particularly for concealing information within multimedia signals such as digital image, audio, or video signals. More particularly, the present invention relates to methods and apparatus for embedding and retrieving information into and out of a digital signal used in multimedia applications while minimizing the effect on the multimedia application of the digital signal.

10

Background and Summary of the Invention

The art of concealing information has existed for millennia and is one to which computers have been readily adapted. It is known, for example, to use computers for encrypting data using various symmetric and asymmetric cryptographic schemes such
15 as the Data Encryption Standard (DES) and RSA encryption, and cryptographic software packages such as PGP (Pretty Good Privacy). Another technique for concealing information for which computers are used is data hiding or steganography, in which the existence of certain information is concealed within a carrier communication. In contrast to cryptography, where it is a goal to make a message undecipherable regardless of its
20 detection, with steganography it is a goal to hide the very existence of the hidden message. An example of a known steganography technique using computers is to embed a digital watermark into a digital image.

According to the present invention, a method of hiding data is provided. A message to be hidden and an encrypting sequence are provided along with a carrier
25 signal that conveys information (unrelated to the message). An encrypted message is generated based on the message and the encrypting sequence. The encrypted message is embedded into the carrier signal by performing an exclusive-OR of the encrypted message with a first portion of the carrier signal.

In preferred embodiments, the carrier signal is a digital image, and the first
30 portion of the carrier signal is an LSB plane of the digital image. The digital image has a plurality of color planes, the first portion of the carrier signal is an LSB plane of a first

-2-

color plane, and the second portion of the carrier signal is an LSB plane of a second color plane.

According to another aspect of the invention, the carrier signal is transmitted to a receiving location. The encrypted message is extracted from the carrier signal and deciphered at the receiving location. In preferred embodiments, the encrypted sequence is generated based on an encrypting key. The encrypted message is generated by performing an exclusive-OR of the message with the encrypting sequence.

According to yet another aspect of the invention, a method of data hiding is provided in which an encryption key and a carrier signal that conveys information unrelated to the encryption key are supplied. An encryption sequence based on the encryption key is generated. The encryption sequence is embedded into the carrier signal.

In preferred embodiments, the encryption key is a public key for an asymmetric encryption algorithm. The carrier signal can be a signal such as a digital image, digital audio, or digital video. The encryption sequence is substantially random, and can be generated based on a linear feedback shift register. The encryption sequence is embedded into the carrier signal by performing an exclusive-OR of the encryption sequence with a portion of the carrier signal.

According to other aspects of the invention, the carrier signal including the embedded encryption sequence is transmitted to a receiving location. The encryption sequence is extracted from the composite signal at the receiving location. The encryption sequence is decrypted to obtain the encryption key. The encryption key is used to generate an encrypted message at the receiving location, and the encrypted message is transmitted from the receiving location.

According to yet another aspect of the invention, a method of data hiding is provided. An encrypted message is embedded into a first portion of a carrier signal and message extraction information is embedded into a second portion of the carrier signal for extracting the encrypted message from the first portion of the carrier signal.

In preferred embodiments, the encrypted message is embedded by performing an exclusive-OR of the encrypted message with the first portion of the carrier signal. The message extraction information is embedded by performing an exclusive-OR of the first portion of the carrier signal with the second portion of the carrier signal. The

first and second portions of the carrier signal can be first and second bit-planes of a digital image.

According to still another aspect of the invention, a method of exchanging data hidden in a carrier signal is provided. A signal including hidden data is generated by transforming a carrier signal from a first domain into a second domain. A message is embedded into the carrier signal in the second domain. The carrier signal is transformed back from the second domain to the first domain. The signal including hidden data is sent to a receiving location. The message is obtained from the signal including hidden data at the receiving location by transforming the signal including hidden data into the second domain and extracting the message.

In preferred embodiments, the message is encrypted prior to generating the signal including hidden data. The message is decrypted after obtaining the message from the signal including hidden data.

According to still yet another aspect of the invention, a data hiding apparatus is provided. An encryption sequence generator generates an encryption sequence based on an encrypting key. An encrypted message generator generates an encrypted message based on the encryption sequence and an input message. An encrypted message embedder embeds the encrypted message into a carrier signal.

In preferred embodiments, the encryption sequence generator generates a substantially random encryption sequence. The encrypted message embedder performs an exclusive-OR of the encrypted message with a portion of the carrier signal. The encrypted message embedder replaces a first LSB plane of a digital image with information based on a second LSB plane of the digital image and performs an exclusive-OR of the encrypted message with the second LSB plane of the digital image. The encrypted message generator performs an exclusive-OR of the input message with the encrypting sequence to generate the encrypted message.

Additional features of the invention will become apparent to those skilled in the art upon consideration of the following detailed description of the preferred embodiments exemplifying the best mode of carrying out the invention as presently perceived.

Brief Description of the Drawings

Fig. 1 is a block diagram of two computer systems connected over a network, each computer system configured with a processor and memory for implementing embodiments of the present invention;

5 Fig. 2 is a flow chart showing a method according to the present invention for hiding data within an image for transmission over a network;

Fig. 3 is a high level block diagram showing a technique for embedding encrypted information into a carrier signal;

10 Fig. 4 is a more detailed block diagram similar to Fig. 3 showing a similar, more specific technique for embedding encrypted information into a carrier signal;

Fig. 5 is a stylized representation of a message format containing embedded, hidden information;

Fig. 6 is a stylized representation similar to Fig. 5 of an alternative message format; and

15 Fig. 7 is a flow chart showing an alternative method according to the present invention for hiding data within an image for transmission over a network.

Detailed Description of the Illustrative Embodiments

The present invention lends itself to implementation in a conventional computer network 10 as shown in Fig. 1. Computer network 10 illustratively includes computer systems 12, 18 connected through a series of network communication devices 14, 16, 20 (e.g., modems, transceivers, etc.) for communication over a network 22 such as the standard telephone lines, or the Internet or World Wide Web. Computer systems 12, 18 are illustratively personal computers and each includes basic elements such as a processor 26, 32, memory 28, 34, storage device 30, 36, and display 31, 38. Computer systems 12, 18 can also include optional peripheral devices such as removable storage device 40 (e.g., a CD-ROM or 3½ inch disk drive).

An exemplary method of data hiding according to the present invention that is suitable for carrying out on computer network 10 is shown in Fig. 2. Although the present invention is disclosed in the context of certain embodiments discussing digital images, other digital signals, such as digital audio or video signals, are also within the scope of the invention.

-5-

According to the method of Fig. 2, an image is used to transport and exchange data that is embedded in the image itself and that cannot be perceived by the human eye. An appropriate analogy is that the image acts as an envelope, with the embedded data transmitted with the image being equivalent to a letter contained within the envelope. Conventional encryption such as PGP or RSA is used to enhance security of the embedded data. The security is improved because the encrypted data is hidden within the image and therefore cannot be recognized as such. This allows for secure data communication and exchange over an insecure transmission channel.

In step 50 an original digital image is obtained. A secret message that is desired to be embedded into the image is generated in step 52. A message encrypting key is used in step 54 to generate an encryption sequence. The message encrypting key can be a seed value for use in generating an m-sequence from a linear feedback shift register as discussed in more detail below, although it is understood that any suitable message encrypting algorithm can be used. As also discussed below, the message encrypting key will ultimately be used by the recipient of the image embedded with the secret message.

In step 56 the secret message from step 52 is encrypted with the encryption sequence from step 54 to create an encrypted message. The encrypted message is then embedded into the image in step 58. There are many methods to embed the encrypted message into the image such as the method discussed below, but, again, it is understood that other suitable methods can be used.

The image with the embedded message is then made available such as on a public network as shown in step 60. Finally, if the secret message from step 52 is actually information that is not desired to be kept secret, such as a public key for an asymmetric encryption algorithm, then the encryption key from step 54 is also made available on the public network as shown in steps 62, 64. This allows for third parties to extract the message from the image. Thus, for example, the message can be a public encryption key that is hidden within the image but that is readily available to a party that has knowledge of the fact that the hidden message exists. This provides a convenient way of exchanging information, such as allowing an individual to make a public encryption key available over the World Wide Web by posting it within an image on a Web site, while still concealing the information from the casual observer.

-6-

It is useful at this point to provide some preliminary definitions before discussing a specific implementation of the method of Fig. 2. The symbol \oplus denotes a bit exclusive-OR function (equivalently, modulo-2 addition). Table 1 illustrates the exclusive-OR function:

5

Table 1

10

<u>A</u>	<u>B</u>	<u>A \oplus B</u>
0	0	0
0	1	1
1	0	1
1	1	0

15

A digital image is typically represented with a two dimensional array of pixel values. If A is the array of pixel values, then $A(x,y)$ denotes the pixel value in the x-th column of the y-th row of the array. Each index x,y begins at zero, and by convention the origin is at the upper-left corner with positive coordinates going rightwards and downwards, although this convention is somewhat arbitrary.

For labeling purposes, it will be assumed that the digital image is a 24-bit RGB image with pixel values ordered as shown in Table 2: xx

Table 2

20

MSB	Red	Green	Blue	LSB
	23 22 21 20 19 18 17 16 R7 R6 R5 R4 R3 R2 R1 R0	15 14 13 12 11 10 9 8 G7 G6 G5 G4 G3 G2 G1 G0	7 6 5 4 3 2 1 0 B7 B6 B5 B4 B3 B2 B1 B0	

25

Thus, bits 16-23 refer to the red component, bits 8-15 refer to the green component, and bits 0-7 refer to the blue component for any given pixel value. For example, $I_{G0}(x,y)$ refers to the least-significant bit of the green component of the (x,y)-pixel in the image I. Since bit G0 is equivalent to bit 8, $I_{G0}(x,y)$ is equivalent to $I_8(x,y)$. As with the array convention, this labeling convention is somewhat arbitrary.

30

An m-sequence is a pseudo-random sequence of binary digits (bits). m-sequences have good statistical properties and can be generated by linear feedback shift registers (configured appropriately as is known in the art). Knowing the size (number of bits), structure (the feedback configuration), and initial fill (the initial contents of each bit) of the shift register allows the reconstruction of the entire m-sequence. The m-sequences here illustratively are generated by a 96-bit m-sequence generator. If the structure and size of the shift register are known (as would be the case with this embodiment), and if a consecutive portion of the m-sequence equal to twice the shift register size is also known,

-7-

the initial fill used to generate the sequence can be determined. In this embodiment the initial fill is used as the key that generates the m-sequence. In this way, the key can be determined from the sequence itself by techniques known to those skilled in cryptography.

When embedding a message into a carrier signal, the order in which pixel operations are performed may be an important consideration. A sequence function $z(i)$ is defined to provide a one-to-one mapping from $i \rightarrow (x,y)$, where i is an ordinal number and (x,y) refers to coordinate values in an image. The ordinal i ranges from zero to $N-1$, where N is the total number of pixels in the image. Given a sequence function $z(i)$, one can compute $z(0), z(1), z(2)$, etc., to obtain a sequence of pixel coordinates $(x_1, y_1), (x_2, y_2)$, etc. As an example, $z(i) = (i \bmod \text{ImageWidth}, \lfloor i / \text{ImageWidth} \rfloor)$ denotes a sequence beginning at the origin and proceeding in a row-by-row fashion.

Given these preliminary definitions, an implementation corresponding to the illustrative method of Fig. 2 of embedding a message into an image is shown by the block diagram in Fig. 3. Input signals are a source image 66 (obtained in step 50), an unencrypted message 68 (generated in step 52), and an encrypting key 70 (used in step 54). Message 68 and encrypting key 70 are processed by an encrypted message generator 76 to create an encrypted message signal 72. Encrypted message 72 is an input along with source image 66 into composite signal generator 78, which creates a composite signal 74 containing source image signal 66 embedded with encrypted message 72.

Composite signal generator 78 illustratively embeds encrypted message 72 into the least-significant bit in the green plane $I_{G0}(x,y)$ of source image 66 to create a new least-significant green bit-plane $I'_{G0}(x,y)$ of composite signal 74. In order subsequently to extract encrypted message 72 from composite signal 74 (I') it will be necessary to know the original values of $I_{G0}(x,y)$ from source image 66. This can of course easily be accomplished by making the original, unmodified image signal 66 available. Composite signal generator 78, however, eliminates the requirement of using original image signal 66 by encoding the original $I_{G0}(x,y)$ into the least-significant red bit-plane $I'_{R0}(x,y)$ of composite signal 74 as discussed below. Thus, in order to extract the embedded encrypted message 72, only composite signal 74 and the encrypting key 70 are needed.

In order to use the method of Figs. 2 and 3 both a sender and receiver of composite signal 74 will need an m -bit shift register with identical feedback configurations and a well-defined ordering function $z(i)$ for any arbitrary image. The following steps

-8-

describe the generation of the composite signal 74 (also referred to as public image I') from original signal 66 (also referred to as original image I), unencrypted message 68 (illustratively a public encryption key, also referred to as K_{PUB}), and encrypting key 70 (also referred to as K_l). As intimated above, encrypting key 70 (K_l) is the initial fill of the
5 m-sequence generator.

In order to generate I' , I' is initially set to be an exact copy of I . I' is then traversed in order $z(i)$ and the red and green least-significant bit planes are set to:

$$I'_{R0}(z(i)) = I'_{G0}(z(i)) \oplus \text{m-seq}(2i)$$

10

$$I'_{G0}(z(i)) = K_{PUB}(i) \oplus I'_{G0}(z(i)) \oplus \text{m-seq}(2i+1)$$

where $K_{PUB}(i)$ refers to the i -th bit of K_{PUB} , and $\text{m-seq}(j)$ refers to the j -th bit in the m-sequence using K_l as the initial fill. With these two equations, information on portion 2 of
15 the image (the green LSB plane) is first placed in portion 1 of the image (the red LSB plane). Then, the message is embedded in portion 2.

To recover K_{PUB} it is only necessary to have the composite signal or public image I' and the encrypting key K_l . For each pixel in I' and in the order $z(i)$, the first step is to extract $I_{G0}^*(z(i))$ by using the least-significant red bit plane and the m-sequence:

20

$$I_{G0}^*(z(i)) = I'_{R0}(z(i)) \oplus \text{m-seq}(2i)$$

$I_{G0}^*(z(i))$ is identical to $I_{G0}(z(i))$ if there are no errors in I' . Then the i -th bit of $K_{PUB}(i)$ is computed by using $I_{G0}^*(z(i))$:

25

$$K_{PUB}^*(i) = I'_{G0}(z(i)) \oplus I_{G0}^*(z(i)) \oplus \text{m-seq}(2i+1)$$

Thus, given K_l , it is possible to reconstruct the same m-sequence used to generate I' . Thus, if no errors occur K_{PUB}^* should be identical to K_{PUB} . Thus, the method of the
30 invention provides for including within the image both the message that is embedded or encrypted in the image as well as the information needed to extract or decrypt the message from the image.

-9-

A more specific method corresponding to an implementation of the method of Figs. 2 and 3 is shown Fig. 4. The same input signals are used, that is, source image 66 (I), message 68 (here, Q instead of K_{PUB}), and encrypting key 70 (K_I) are used. The primary refinement in the method of Fig. 4 as compared with Fig. 3 is an encoding process to handle varying length messages 68.

Message 68, which in the example of Fig. 3 was a public encryption key for use in an asymmetric cryptography system, can more generally simply be a collection of bits intended to be encrypted and is referred to here as Q. The length (i.e., the total number of bits) of Q is denoted $|Q|$. The i-th bit of the message Q is denoted $Q(i)$, where the bits are numbered from 0 to $|Q|-1$.

Message 68 (Q) is an input signal to message generator 82 which has as a second input the output from a random noise generator 84. Random noise generator 84 illustratively is also a 96-bit m-sequence generator using an initial fill of a computer system time value, although other suitable random signal generators can be used.

Encrypting key 70 (K_I) is an input signal (initial fill) to an m-sequence generator 80 that illustratively is the same as random noise generator 84, which then generates as an output an encrypting sequence 86.

Unless the message 68 (Q) will always be the same length (in bits) and that length is the number of pixels in the source image, it will not be possible to embed Q directly onto source image 66 (I). It is therefore necessary to encode additional information that will enable subsequent extraction of messages Q of varying sizes from composite signal 74 (I'). Thus, the message 88 to be encoded onto image 66 (I) is generated by message generator 82 with special properties and is denoted Q' to show that it is derived from Q.

Q' has the following properties. For any given source image I, regardless of what message Q is being encoded, the size of a message Q' is the same as the total number of pixels in image I (that is, $|Q'| = \# \text{ pixels in } I$). The bits of message Q' are labeled according to standard convention, that is, the first bit (or the left-most bit if Q' is viewed as an ordered bit stream from left to right as shown in Fig. 5) is numbered zero. Thus the bits of Q' are numbered from zero to $|Q'|-1$.

The structure of Q' is shown in Fig. 5. All bits except the last sixty-four form a data area 92. The last sixty-four bits consist of two thirty-two bit words (StartPos

-10-

and Length, in that order), which form a Trailer. Data area 92 includes data bits 98 that correspond to the message Q itself, and random bits 97, 99 that help hide the location of Q (bits 98) within Q'. As part of the encoding process, message generator 82 computes the length of message Q and stores its value in the final 32 bits 94 of the Trailer. The 5 value of the length is not directly encoded and instead a value congruent (actual length modulo Data Area size) is placed in the 32-bit word. It is trivial to recover the length from this encoded value.

Starting position 94 describes the location within data area 92 where the bits of the message Q reside. Message generator 82 randomly chooses a place 98 to store 10 Q and populates all other bits of unused portions 97, 99 in data area 92 with random noise generated by random noise generator 84. Thus, Q can be anywhere in data area 92. Including noise for portions 97, 99 of data area 92 unused by message Q improves security of data embedded within I because the noise increases the difficulty of recognizing the existence or location of Q within the data area.

15 The encoding of each bit of message Q' is encoded onto image I on a one-bit per one-pixel basis using an exclusive-OR as discussed above for the method of Fig. 3. First, the output of m-sequence generator 80 (with K_1 as a seed value) is used to encrypt Q' in encrypter 90. Next, the encrypted Q' is embedded onto the LSB green plane I_{G0} . Encrypted message Q is subsequently extracted from Q' by locating its starting position 20 and length from the trailer. The extracted Q is then decoded as discussed above.

Further implementation steps can be taken to increase security for message 25 Q'. Random number generator 84 and m-sequence generator 80 can be different. Even if both use 96-bit m-sequence generators, this can be achieved simply by changing the feedback coefficients. Moreover, the message length 94 in the trailer can be relocated to data area 92 as shown in Fig. 6. This relocation will limit the ability of an attacker to take advantage of a known size of message Q.

Another way to provide for security of data hidden within a carrier image is shown by the method of Fig. 7. In step 102 the carrier image is transformed from a first domain to a second domain. For example, a typical RGB image that is considered to be 30 represented in a spatial domain can be transformed using a discrete cosine transform. A message is then embedded into the transformed carrier image in step 104, using any appropriate technique for embedding a message onto a carrier signal. An example of a

-11-

transformed image into which a message can be embedded would be a JPEG image. If desired, the message can also be pre-encrypted before being embedded into the transformed image to further improve security. The image is then transformed back into the first domain in step 106 and made available for access by third parties in step 108.

5 For a third party to extract the message the steps are essentially reversed. First the image is copied by the third party in step 110, and it is then transformed into the second domain in step 112 using the same transform performed in step 106. Finally, the message is extracted in step 114, again, using any appropriate technique that corresponds to the technique used in step 104 for originally embedding the message. If the message
10 was pre-encrypted then another decryption step (not shown) will be necessary.

Encrypted messages relying on the use of encryption keys are used in the methods discussed above. For example, if a pre-encrypted message is embedded into an image, then the recipient will need a key to decrypt the message. A technique for providing for secure exchanges of encrypted data such as encryption keys that is known in
15 the art is the use of a trusted third party. The trusted third party essentially acts as a secure broker in exchanging data between two other parties. It is within the scope of this invention to exchange information, such as encryption keys, by use of a trusted third party.

Although the invention has been described in detail with reference to
20 certain illustrated embodiments, variations and modifications exist within the scope and spirit of the present invention as described and defined in the following claims.

CLAIMS:

1. A method of data hiding comprising the steps of:
 - providing a message;
 - 5 providing an encrypting sequence;
 - generating an encrypted message based on the message and the encrypting sequence;
 - providing a carrier signal that conveys information unrelated to the encrypted message; and
- 10 embedding the encrypted message into the carrier signal by performing an exclusive-OR of the encrypted message with a first portion of the carrier signal.
2. The method of claim 1, wherein the carrier signal is a digital image.
3. The method of claim 2, wherein the first portion of the carrier signal is an LSB plane of the digital image.
- 15 4. The method of claim 1, further comprising the step of embedding the first portion of the carrier signal into a second portion of the carrier signal.
5. The method of claim 4, wherein the carrier signal is a digital image having a plurality of color planes, the first portion of the carrier signal is an LSB plane of a first color plane, and the second portion of the carrier signal is an LSB plane of a second color plane.
- 20 6. The method of claim 1, further comprising the steps of transmitting the composite signal to a receiving location, extracting the encrypted message from the composite signal at the receiving location, and decrypting the encrypted message at the receiving location.
- 25 7. The method of claim 1, wherein the step of generating an encrypted message includes generating the encrypting sequence based on an encrypting key and performing an exclusive-OR of the message with the encrypting sequence to generate the encrypted message.
8. The method of claim 7, further comprising the steps of transmitting the composite signal to a receiving location, extracting the encrypted message from the composite signal at the receiving location, and decrypting the encrypted message at the receiving location based on the encrypting key.

-13-

9. The method of claim 1, wherein the step of providing a message comprised of providing a pre-encrypted message.

10. The method of claim 9, further comprising the step of exchanging an encryption key for decrypting the pre-encrypted message using a trusted third party.

5 11. A method of data hiding comprising the steps of:
providing an encryption key;
generating an encryption sequence based on the encryption key;
providing a carrier signal that conveys information unrelated to the
encryption key; and

10 embedding the encryption sequence into the carrier signal.

12. The method of claim 11, wherein the encryption key is a public key for an asymmetric encryption algorithm.

13. The method of claim 11, wherein the carrier signal is selected from the group comprising digital images, digital audio, and digital video.

15 14. The method of claim 11, wherein the encryption sequence is substantially random.

15. The method of claim 14, wherein the encryption sequence is generated based on a linear feedback shift register.

20 16. The method of claim 11, wherein the step of embedding the encryption sequence includes performing an exclusive-OR of the encryption sequence with a portion of the carrier signal.

25 17. The method of claim 11, further comprising the steps of transmitting the carrier signal including the embedded encryption sequence to a receiving location, extracting the encryption sequence from the composite signal at the receiving location, and deciphering the encryption sequence to obtain the encryption key at the receiving location.

18. The method of claim 17, further comprising the steps of encrypting a message using the encryption key to generate an encrypted message at the receiving location and transmitting the encrypted message from the receiving location.

30 19. A method of data hiding comprising the steps of:
embedding an encrypted message into a first portion of a carrier signal;
and

-14-

embedding message extraction information into a second portion of the carrier signal for extracting the encrypted message from the first portion of the carrier signal.

20. The method of claim 19, wherein the step of embedding an
5 encrypted message includes performing an exclusive-OR of the encrypted message with the first portion of the carrier signal.

21. The method of claim 20, wherein the step of embedding message extraction information includes performing an exclusive-OR of the first portion of the carrier signal with the second portion of the carrier signal.

10 22. The method of claim 21, wherein the first and second portions of the carrier signal are first and second bit-planes of a digital image.

23. A method of exchanging data hidden in a carrier signal comprising the steps of:

15 generating a signal including hidden data by transforming a carrier signal from a first domain into a second domain, embedding a message into the carrier signal in the second domain, and transforming the carrier signal back from the second domain to the first domain;

sending the signal including hidden data to a receiving location; and
obtaining the message from the signal including hidden data at the
20 receiving location by transforming the signal including hidden data into the second domain and extracting the message.

24. The method of claim 23, further comprising the steps of encrypting the message prior to generating the signal including hidden data and decrypting the message after obtaining the message from the signal including hidden data.

25. A data hiding apparatus comprising:
an encryption sequence generator configured to generate an encryption sequence based on an encrypting key;
an encrypted message generator configured to generate an encrypted message based on the encryption sequence and an input message; and
30 an encrypted message embedder configured to embed the encrypted message into a carrier signal.

-15-

26. The method of claim 25, wherein the encryption sequence generator is configured to generate a substantially random encryption sequence.

27. The method of claim 25, wherein the encrypted message generator is configured to perform an exclusive-OR of the input message with the encrypting sequence to generate the encrypted message.

28. The method of claim 25, wherein the encrypted message embedder is configured to perform an exclusive-OR of the encrypted message with a portion of the carrier signal.

29. The method of claim 28, wherein the encrypted message embedder 10 is configured to replace a first LSB plane of the digital image with information based on a second LSB plane of the digital image and to perform an exclusive-OR of the encrypted message with the second LSB plane of the digital image.

1 / 4

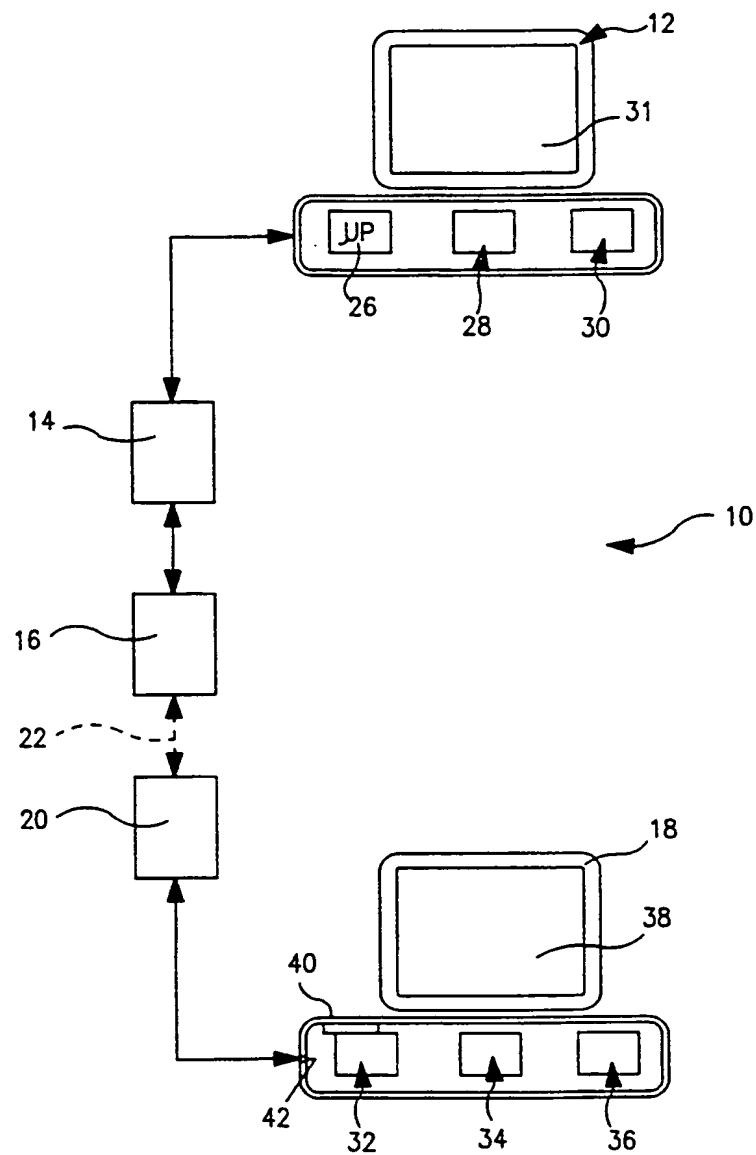


FIG. 1

2 / 4

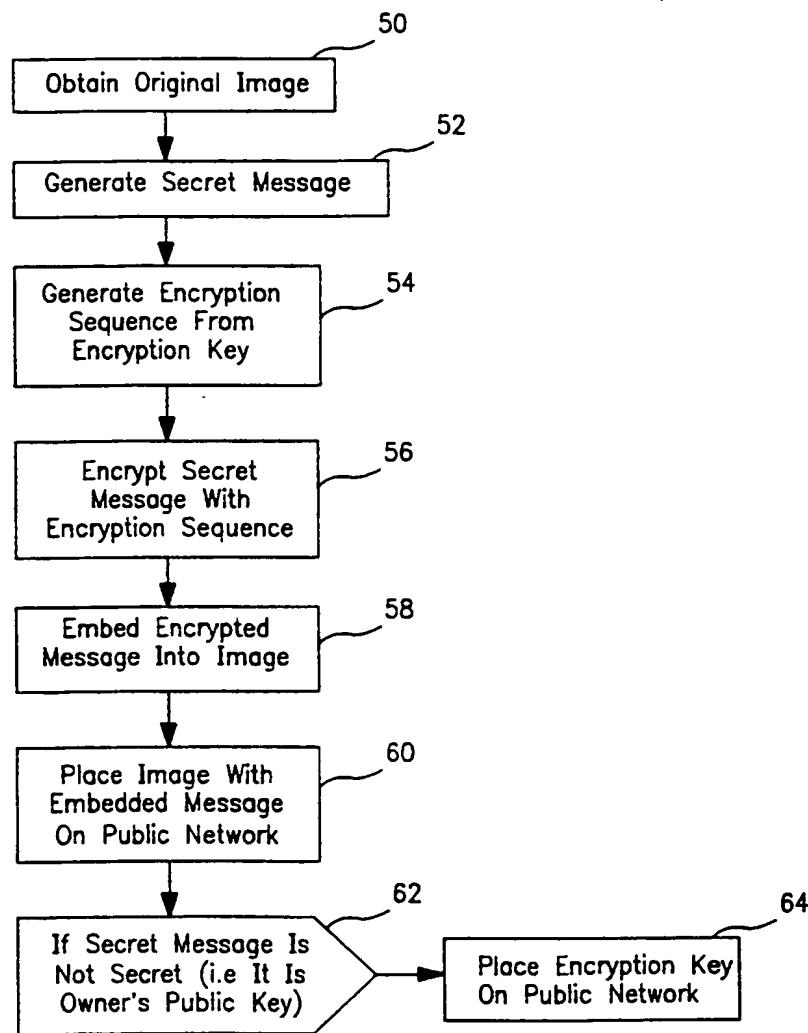


FIG. 2

3 / 4

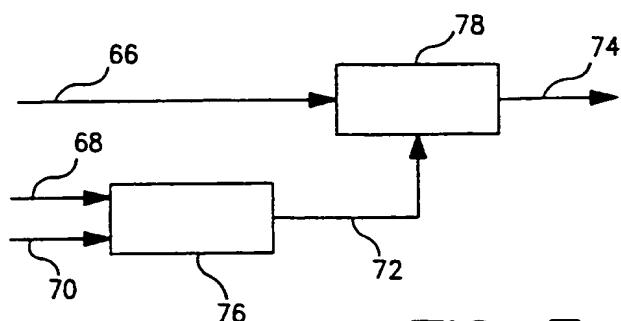


FIG. 3

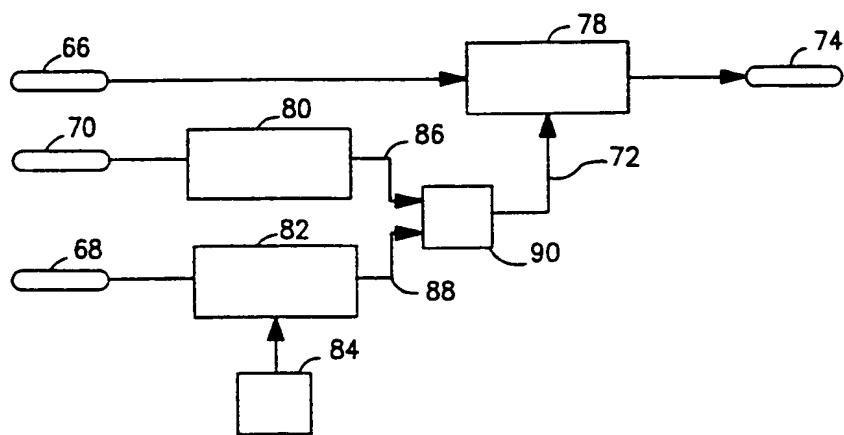


FIG. 4

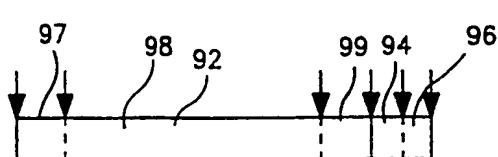


FIG. 5

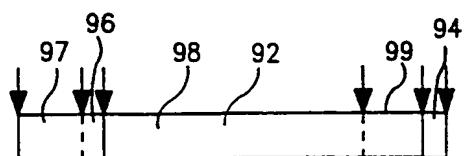


FIG. 6

4 / 4

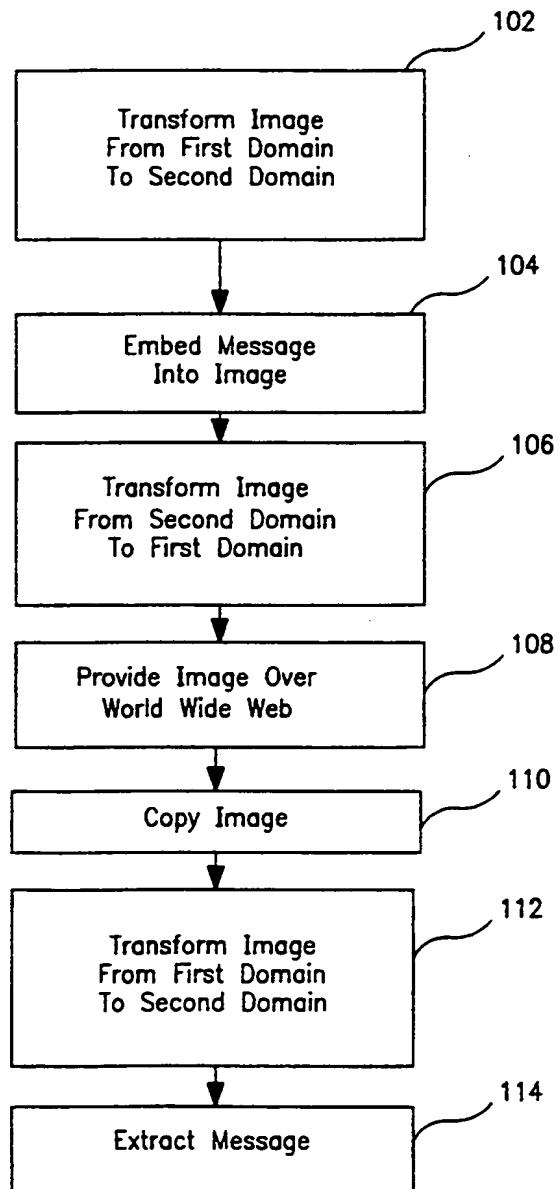


FIG. 7

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 98/17321

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04L9/00 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>YASUHIRO NAKAMURA ET AL: "A UNIFIED CODING METHOD OF DITHERED IMAGE AND TEXT DATA USING MICROPATTERNS" ELECTRONICS & COMMUNICATIONS IN JAPAN, PART I - COMMUNICATIONS, NEW YORK (US), vol. 72, no. 4, PART 01, 1 April 1989, pages 50-56, XP000080029 see page 50, left-hand column, last paragraph - right-hand column, line 18 see page 55, left-hand column, paragraph 4 - right-hand column, paragraph 1</p> <p>---</p> <p style="text-align: center;">-/--</p>	11,13,25



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

5 February 1999

Date of mailing of the international search report

15/02/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 98/17321

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 359 325 A (KONINKL PHILIPS ELECTRONICS NV) 21 March 1990 see abstract see column 2, line 11 - line 34 see column 3, line 1 - line 18 see column 3, line 39 - line 48 see column 4, line 30 - column 5, line 22 see column 5, line 39 - line 50 see column 7, line 46 - column 8, line 5 ---	1,3,16, 19,20
A	US 5 195 136 A (HARDY DOUGLAS A ET AL) 16 March 1993 see column 4, line 21 - line 54 ---	1,14-16, 26,27
P,X	COX I J ET AL: "SECURE SPREAD SPECTRUM WATERMARKING FOR MULTIMEDIA" IEEE TRANSACTIONS ON IMAGE PROCESSING, NEW YORK (US), vol. 6, no. 12, December 1997, pages 1673-1687, XP000199950 see page 1677, right-hand column, line 7 - page 1678, left-hand column, line 10 ---	23
X	PODILCHUK C I ET AL: "DIGITAL IMAGE WATERMARKING USING VISUAL MODELS" PROCEEDINGS OF THE SPIE, vol. 3016, 10 February 1997, pages 100-111, XP000199957 see page 103, line 22 - page 104, line 11; figure 1 -----	23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 98/17321

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP 0359325	A 21-03-1990	NL	8802291 A	17-04-1990
		DE	68919958 D	26-01-1995
		DE	68919958 T	29-06-1995
		DE	68928493 D	22-01-1998
		DE	68928493 T	04-06-1998
		EP	0545915 A	09-06-1993
		HK	76796 A	10-05-1996
		JP	2119446 A	07-05-1990
		US	5146457 A	08-09-1992
US 5195136	A 16-03-1993	NONE		

Express Mail No. EM466245407US

PATENT COOPERATION TREATY

21

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
BARNES & THORNBURG
Attn. NIEDNAGEL, T.
11 South Meridian Street
Suite 1313
INDIANAPOLIS, INDIANA 46204
UNITED STATES OF AMERICA

RECEIVED

FEB 26 1999

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT
OR THE DECLARATION

(PCT Rule 44.1)

BARNES & THORNBURG

SEARCHED

SECRET

TX
31/08/1998

Date of mailing
(day/month/year)

15/02/1999

Applicant's or agent's file reference:

3220-60866

FOR FURTHER ACTION

See paragraphs 1 and 4 below

International application No.

PCT/US 98/17321

International filing date

(day/month/year)

21/08/1998

Applicant

PURDUE RESEARCH FOUNDATION et al.

SEARCHED

31/08/1998

COPY: ST

1. The applicant is hereby notified that the International Search Report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19

The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the International Search Report; however, for more details, see the notes on the accompanying sheet.

Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Fascimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. The applicant is hereby notified that no International Search Report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after 18 months from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.

Within 19 months from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within 20 months from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the International Searching Authority

European Patent Office, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040. Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Authorized officer

René Stolk

INTERNATIONAL COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 3220-60866	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/US 98/ 17321	International filing date (day/month/year) 21/08/1998	(Earliest) Priority Date (day/month/year) 22/08/1997
Applicant PURDUE RESEARCH FOUNDATION et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.
 It is also accompanied by a copy of each priorart document cited in this report.

1. Certain claims were found unsearchable (see Box I).
2. Unity of invention is lacking (see Box II).
3. The international application contains disclosure of a nucleotide and/or amino acid sequence listing and the international search was carried out on the basis of the sequence listing
 - filed with the international application.
 - furnished by the applicant separately from the international application,
 - but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in the international application as filed.
 - Transcribed by this Authority
4. With regard to the title, the text is approved as submitted by the applicant
 the text has been established by this Authority to read as follows:
Hiding of encrypted data
5. With regard to the abstract,
 - the text is approved as submitted by the applicant
 - the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this International Search Report, submit comments to this Authority.
6. The figure of the drawings to be published with the abstract is:
 Figure No. 4
 - as suggested by the applicant.
 - because the applicant failed to suggest a figure.
 - because this figure better characterizes the invention.

None of the figures.

Express Mail No. EM4662454074S

PATENT COOPERATION TRE

Kat
26/08/94

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

NIEDNAGEL, T.
BARNES & THORNBURG
11 South Meridian Street
Suite 1313
INDIANAPOLIS, INDIANA 46204
ETATS-UNIS D'AMERIQUE

OCT 27 1999

BARNES & THORNBURG

PCT

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL PRELIMINARY
EXAMINATION REPORT

(PCT Rule 71.1)

Date of mailing
(day/month/year)

2 i. 10. 99

Applicant's or agent's file reference
3220-60866

IMPORTANT NOTIFICATION

International application No.
PCT/US98/17321

International filing date (day/month/year)
21/08/1998

Priority date (day/month/year)
22/08/1997

Applicant
PURDUE RESEARCH FOUNDATION et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. REMINDER

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized officer

Ahrens, R

Tel. +49 89 2399-8136



PATENT COOPERATION TREATY

REC'D 25 OCT 1999

WIPO

PCT

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 3220-60866	FOR FURTHER ACTION		See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US98/17321	International filing date (day/month/year) 21/08/1998	Priority date (day/month/year) 22/08/1997	
International Patent Classification (IPC) or national classification and IPC H04L9/00			
Applicant PURDUE RESEARCH FOUNDATION et al.			
<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of 9 sheets, including this cover sheet.</p> <p><input type="checkbox"/> This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of sheets.</p>			
<p>3. This report contains indications relating to the following items:</p> <ul style="list-style-type: none"> I <input checked="" type="checkbox"/> Basis of the report II <input checked="" type="checkbox"/> Priority III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability IV <input checked="" type="checkbox"/> Lack of unity of invention V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement VI <input type="checkbox"/> Certain documents cited VII <input checked="" type="checkbox"/> Certain defects in the international application VIII <input checked="" type="checkbox"/> Certain observations on the international application 			

Date of submission of the demand 08/03/1999	Date of completion of this report 21.10.99
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Snell, T Telephone No. +49 89 2399 8802



**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/US98/17321

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-11 as originally filed

Claims, No.:

1-29 as originally filed

Drawings, sheets:

1/4-4/4 as originally filed

2. The amendments have resulted in the cancellation of:

the description, pages:
 the claims, Nos.:
 the drawings, sheets:

3. This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

II. Priority

1. This report has been established as if no priority had been claimed due to the failure to furnish within the prescribed time limit the requested:
 - copy of the earlier application whose priority has been claimed.
 - translation of the earlier application whose priority has been claimed.
2. This report has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid.

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/US98/17321

Thus for the purposes of this report, the international filing date indicated above is considered to be the relevant date.

3. Additional observations, if necessary:

see separate sheet

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

- restricted the claims.
- paid additional fees.
- paid additional fees under protest.
- neither restricted nor paid additional fees.

2. This Authority found that the requirement of unity of invention is not complied and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

- complied with.
- not complied with for the following reasons:

see separate sheet

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

- all parts.
- the parts relating to claims Nos. .

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/US98/17321

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims 1-10, 12-24, 26-29
	No:	Claims 11, 25
Inventive step (IS)	Yes:	Claims
	No:	Claims 1-29
Industrial applicability (IA)	Yes:	Claims 1-29
	No:	Claims

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/US98/17321

Cited documents

D1: YASUHIRO NAKAMURA ET AL: 'A UNIFIED CODING METHOD OF DITHERED IMAGE AND TEXT DATA USING MICROPATTERNS' ELECTRONICS & COMMUNICATIONS IN JAPAN, PART I - COMMUNICATIONS, NEW YORK (US), vol. 72, no. 4, PART 01, 1 April 1989, pages 50-56

D2: EP-A-0 359 325 (KONINKL PHILIPS ELECTRONICS NV) 21 March 1990

D3: PODILCHUK C I ET AL: 'DIGITAL IMAGE WATERMARKING USING VISUAL MODELS' PROCEEDINGS OF THE SPIE, vol. 3016, 10 February 1997, pages 100-111

D4: COX I J ET AL: 'SECURE SPREAD SPECTRUM WATERMARKING FOR MULTIMEDIA' IEEE TRANSACTIONS ON IMAGE PROCESSING, NEW YORK (US), vol. 6, no. 12, December 1997, pages 1673-1687

Re Item II

Priority

1. If the priority of the application were invalid, document D4 would be relevant in respect of novelty and inventive step for claims 23 and 24.

Re Item IV

Lack of unity of invention

1. Claims 1-22 and 25-29 (first invention) relate broadly to a method or apparatus for data hiding including embedding a message in a carrier by performing an exclusive-OR operation.

Claims 23 and 24 (second invention) refer on the other hand to an embodiment involving embedding a message in a carrier by transforming a carrier signal from a first domain into a second domain, embedding the message, and transforming

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/US98/17321

the carrier signal back to the first domain.

Since several documents (see D1, D2, D3) already disclose the common concept between these two inventions of data hiding including embedding a message in a carrier, there is no common concept linking the special technical feature of an exclusive-OR operation on the one hand and performing a carrier transformation on the other.

The requirements of unity of invention are therefore not met (Rules 13.1 and 13.2 PCT).

Re Item V

Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. With respect to claim 1, D2 discloses a method of data hiding comprising the steps of:

providing a message (d);
providing a carrier signal (b0-b7) that conveys information unrelated to the encrypted message; and
embedding the message into the carrier signal by performing an exclusive-OR of the encrypted message with a first portion of the carrier signal (see col. 5, lines 1-5).

The subject-matter of claim 1 differs from D2 only in the fact that the message is encrypted based on an encryption sequence.

This difference relates to the problem of providing security of transmission.

However, considering that this problem has been solved in a similar environment in D1, ie D1 discloses the principle of data hiding by embedding an encrypted message into a carrier (see fig. 7), it would be obvious to for a person skilled in

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/US98/17321

the art to modify the method of D2 to include the step of encrypting the message to provide the advantages of security of transmission, and thus to arrive without the exercise of an inventive step at the subject-matter of claim 1.

Claim 1 therefore does not meet the requirements of Articles 33(1) and (3) PCT.

2. With respect to claim 11, D1 discloses a method of data hiding comprising the steps of (see fig. 7):

providing an encryption key (fig. 7, "key");

generating an encryption sequence based on the encryption key (fig. 7, "encryption"); and

providing a carrier signal that conveys information unrelated to the encryption key (Image data, see page 50, left-hand col. last paragraph to right-hand col., line 2 and page 55, section 6).

D1 therefore discloses all the features of claim 11; the subject-matter of claim 11 is therefore not novel (Articles 33(1) and (2) PCT).

3. Claim 25 corresponds for the apparatus category to method claim 11; its subject-matter is therefore also not novel for the same reasons as claim 11 (Articles 33(1) and (2) PCT).
3. If novelty should be disputed based on some minor difference of interpretation, it is pointed out that the subject-matter of these claims would in any case not involve an inventive step (Article 33(3) PCT), given that D1 attempts to solve the same problem and describes the same type of solution as presently claimed.
4. Independent claim 19 differs from claim 1 in that message extraction information is embedded in a second portion of the carrier signal for extracting the encrypted message.

This difference does not involve an inventive step, being rendered obvious by D2, where bit b7, which is embedded in the message, is used to extract the message in the receiver.

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/US98/17321

The subject-matter of claim 19 therefore does not involve an inventive step (Articles 33(1) and (3) PCT).

5. The additional features of dependent claims 2-10, 12-18, 20-22 and 26-29 add nothing of inventive significance to claims 1, 11, 19 or 25, being either disclosed or obviously derivable from either D1 or D2 (see the passages cited in the search report, and D2, col. 3, lines 39-42) (Article 33(3) PCT).
6. With respect to claim 23, D3 discloses a method of exchanging data hidden in a carrier signal comprising the steps of:

generating a signal including hidden data ("watermark sequence") by transforming a carrier signal from a first domain into a second domain (see page 103, section 4.1), embedding a message into the carrier signal in the second domain (see figure 1, "Encoder");

sending the signal including hidden data to a receiving location; and obtaining the message from the signal including hidden data at the receiving location by transforming the signal including the hidden data into the second domain and extracting the message (see figure 1, "Decoder").

The only difference between the subject-matter of claim 23 and D3 lies in the fact that D3 does not explicitly show the carrier signal being transformed back to the first domain; this step is however obvious to enable the watermarked image to be viewed (figure 2); moreover the input to the decoder is the watermarked image, ie in the first domain, so at some point the signal has been transformed back into the first domain.

The subject-matter of claim 23 therefore does not involve an inventive step (Articles 33(1) and (3) PCT).

7. The additional feature of claim 24 adds nothing of inventive significance to claim 23 having regard to figure 7 of D1 (Article 33(3) PCT).

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/US98/17321

Re Item VII

Certain defects in the international application

1. The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).
2. Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1-D3 is not mentioned in the description, nor are these documents identified therein.

Re Item VIII

Certain observations on the international application

1. The plurality of independent claims in the method category (claims 1, 11, 19, 23 and 25) comprising varying combinations of features render the set of claims as a whole not clear and concise, and makes it impossible for a third party to determine the scope of protection sought due to the total lack of consistency between the independent claims in defining the essential features of the invention.

Claims 1, 11, 19, 23 and 25 therefore do not meet the requirements of Article 6 PCT.

2. The statement in the description on page 11, lines 19-21 ("spirit of the invention") implies that the subject-matter for which protection is sought may be different to that defined by the claims, thereby resulting in lack of clarity of the claims (Article 6 PCT) when the description is used to interpret them (see also the PCT Guidelines, PCT/GL/3 III, 4.3a).
3. Method claims 26-29 are dependent on claim 25, which is a claim for an apparatus, leading to a lack of clarity in the scope of protection sought (Article 6 PCT).

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 98/17321

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/00 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>YASUHIRO NAKAMURA ET AL: "A UNIFIED CODING METHOD OF DITHERED IMAGE AND TEXT DATA USING MICROPATTERNS" ELECTRONICS & COMMUNICATIONS IN JAPAN, PART I - COMMUNICATIONS, NEW YORK (US), vol. 72, no. 4, PART 01, 1 April 1989, pages 50-56, XP000080029 see page 50, left-hand column, last paragraph - right-hand column, line 18 see page 55, left-hand column, paragraph 4 - right-hand column, paragraph 1</p> <p>---</p> <p style="text-align: center;">-/--</p>	11,13,25

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

° Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

5 February 1999

15/02/1999

Name and mailing address of the ISA
 European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel: (+31-70) 340-2040, Tx. 31 651 epo nl.
 Fax: (+31-70) 340-3016

Authorized officer

Holper, G

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/US 98/17321

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 359 325 A (KONINKL PHILIPS ELECTRONICS NV) 21 March 1990 see abstract see column 2, line 11 - line 34 see column 3, line 1 - line 18 see column 3, line 39 - line 48 see column 4, line 30 - column 5, line 22 see column 5, line 39 - line 50 see column 7, line 46 - column 8, line 5 ---	1, 3, 16, 19, 20
A	US 5 195 136 A (HARDY DOUGLAS A ET AL) 16 March 1993 see column 4, line 21 - line 54 ---	1, 14-16, 26, 27
P, X	COX I J ET AL: "SECURE SPREAD SPECTRUM WATERMARKING FOR MULTIMEDIA" IEEE TRANSACTIONS ON IMAGE PROCESSING, NEW YORK (US), vol. 6, no. 12, December 1997, pages 1673-1687, XP000199950 see page 1677, right-hand column, line 7 - page 1678, left-hand column, line 10 ---	23
X	PODILCHUK C I ET AL: "DIGITAL IMAGE WATERMARKING USING VISUAL MODELS" PROCEEDINGS OF THE SPIE, vol. 3016, 10 February 1997, pages 100-111, XP000199957 see page 103, line 22 - page 104, line 11; figure 1 -----	23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 98/17321

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0359325 A	21-03-1990	NL 8802291 A DE 68919958 D DE 68919958 T DE 68928493 D DE 68928493 T EP 0545915 A HK 76796 A JP 2119446 A US 5146457 A	17-04-1990 26-01-1995 29-06-1995 22-01-1998 04-06-1998 09-06-1993 10-05-1996 07-05-1990 08-09-1992
US 5195136 A	16-03-1993	NONE	



DOCUMENTS CONSIDERED TO BE RELEVANT									
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl. 5)						
A	GB-A-1 203 768 (MINISTRY OF TECHNOLOGY) * Page 1, left-hand column, lines 27-46; page 2, left-hand column, line 44 - page 3, left-hand column, line 12; page 4, right-hand column, lines 109-120; page 7, right-hand column, line 115 - page 8, right-hand column, line 5 * --- A GB-A-2 149 560 (PHILIPS) * Page 1, lines 45-65 * --- A GB-A-2 063 018 (GENERAL ELECTRIC) * Page 1, left-hand column, lines 34-50; figure * -----	1,4,6-8 1,2 1	H 04 J 3/12 G 11 B 20/18						
			TECHNICAL FIELDS SEARCHED (Int. Cl. 5)						
			H 04 J H 04 Q G 11 B						
<p>The present search report has been drawn up for all claims</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;">Place of search</td> <td style="width: 33%;">Date of completion of the search</td> <td style="width: 34%;">Examiner</td> </tr> <tr> <td>THE HAGUE</td> <td>31-10-1989</td> <td>VAN DEN BERG, J.G.J.</td> </tr> </table>				Place of search	Date of completion of the search	Examiner	THE HAGUE	31-10-1989	VAN DEN BERG, J.G.J.
Place of search	Date of completion of the search	Examiner							
THE HAGUE	31-10-1989	VAN DEN BERG, J.G.J.							
CATEGORY OF CITED DOCUMENTS		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document							
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document									